

Ομάδες, Στατιστική Απόσταση & Pedersen

1. Χρησιμοποιούμε δεσμεύσεις Pedersen για να υλοποιήσουμε τη ρίψη νομισμάτων. Στη συνηθισμένη εφαρμογή των δεσμεύσεων, ο πρώτος παίκτης αντί να φανερώσει το κέρμα του φανερώνει μια δέσμευση, την οποία ανοίγει αφού φανερώσει την τιμή του ο δεύτερος παίκτης.

Κάποιος προτείνει να αλλάξουμε το πρωτόκολλο ως εξής για μεγαλύτερη ασφάλεια: ο δεύτερος παίκτης, αντί να αποκαλύψει άμεσα την τιμή b , θα δώσει μία δέσμευση σε αυτήν. Κατόπιν, ο πρώτος παίκτης ανοίγει τη δεσμευσή του, μετά ο δεύτερος τη δική του και το πρωτόκολλο τερματίζει κατά τα γνωστά. Οι παράμετροι για το σχήμα του Pedersen υποθέτουμε εδώ ότι προήλθαν από έμπιστο τρίτο πρόσωπο.

Γνωρίζοντας από την προηγούμενη εβδομάδα ότι αυτή η παραλλαγή είναι ευπαθής σε replay attacks, εάν ο δεύτερος παίκτης απλώς επαναλάβει τη δέσμευση του πρώτου, θεωρούμε ότι χάνει χωρίς να υπολογίσουμε το XOR.

Εξετάστε την περίπτωση της παραπάνω αλλαγής στο πρωτόκολλο (πέρα από την ανάγκη για την ύπαρξη του τρίτου προσώπου).

2. Να υπολογίσετε το $123^{2022} \bmod 23$.
3. Να υπολογίσετε (προσεγγιστικά) το $\log_{10}(123456789012345678901234567890)$ καθώς και το $\log_2(123456789012345678901234567890)$. Δίνεται ότι $\log_2(10) \approx 3.3$
4. Να υπολογίσετε το $\log_2 5 \bmod 37$. Χρησιμοποιείτε τον αλγόριθμο Baby step, Giant step, ο οποίος δίνεται παρακάτω.

Στον αλγόριθμο Baby step, Giant step, θέλουμε να λύσουμε την εξίσωση $g^x = h \bmod p$ «σπάζοντας» τον άγνωστο λογάριθμο $0 \leq x < p - 1$ σε $x = b + S \cdot G$, όπου $S = \lceil \sqrt{(p-1)} \rceil$ και $b, G \leq S$.

Για να το κάνουμε αυτό, ξαναγράφουμε την εξίσωση ως $g^{S \cdot B} \equiv h \cdot g^{-b}$, με αγνώστους το B και το b . Έτσι, μπορούμε να εξαντλήσουμε όλες τις περιπτώσεις, με $2S$ υπολογισμούς (και $O(n \log n)$ συγκρίσεις για ταξινόμηση), αντί τους $p - 1 = S^2$ υπολογισμούς της προφανούς λύσης.

Παρατήρηση. Επειδή το 37 είναι πρώτος και $37 - 1 = 36$, η τάξη της πολλαπλασιαστικής ομάδας του \mathbb{Z}_{37}^* είναι 36. Η τάξη του 2 ξέρουμε ότι διαιρεί το 36 και άρα υπάρχουν πολλές μη τετριμμένες περιπτώσεις για την τάξη του. Σε περίπτωση που η τάξη του 2 δεν είναι 36, τότε δεν παράγει όλη την ομάδα, άρα ενδέχεται το 5 να μην εμφανιστεί ως δύναμή του, και ο ζητούμενος λογάριθμος να μην υπάρχει.

5. Η Καρολίνα και ο Λυκούργος χρησιμοποιούν το σχήμα δέσμευσης του Pedersen. Η Καρολίνα έχει ορίσει τις παραμέτρους και ο Λυκούργος της έχει στείλει τη δέσμευση c . Πριν γίνει οτιδήποτε άλλο, ο Λυκούργος διαπιστώνει ότι από τυπογραφικό λάθος στις σημειώσεις του, υπολόγισε την τιμή $g^m h^r$ αντί $g^r h^m$. Είναι δυνατό με τις ανάλογες διορθώσεις από τη μεριά της Καρολίνας να συνεχίσουν την επικοινωνία τους ή πρέπει ο Λυκούργος να δημιουργήσει νέα δέσμευση;
6. Ο Λυκούργος αποφασίζει για καλό και για κακό να δημιουργήσει νέα δέσμευση c' έχοντας διορθώσει το λάθος στον υπολογισμό, αλλά για οικονομία χρόνου επαναχρησιμοποιεί την ίδια τιμή r . Δεδομένου ότι δεσμεύεται στο ίδιο μήνυμα με πριν (άρα και η τιμή m είναι ίδια), είναι σωστή η απόφασή του;
7. Για τους παρακάτω αλγορίθμους, να υπολογιστεί η στατιστική απόσταση της εξόδου τους από την ομοιόμορφη κατανομή U στο $S = \{0, 1, 2, \dots, A - 1\}$.

Sampler 1. $n := \lceil \log_2 A \rceil$
 $x_0, x_1, \dots, x_{n-1} \leftarrow \{0, 1\}$
 $y := \sum_{i=0}^{n-1} 2^i \cdot x_i$
return y

Sampler 2. $x_0, x_1, \dots, x_{A-1} \leftarrow \{0, 1\}$
 $y := \sum_{i=0}^{A-1} x_i$
return y

Υπόδειξη: Γνωρίζουμε ότι για τη διωνυμική ο μέσος όρος $E(X)$ είναι $n \cdot p = \frac{A}{2}$, και η διακύμανση $Var[X]$ είναι $n \cdot p \cdot q = \frac{A}{4}$. Επιπλέον, από τις σημειώσεις, ανατρέξτε στην ανισότητα του Chebychev (2.5.2):

$$\Pr[| - E() | \geq t] \leq \frac{Var[]}{t^2}$$

Sampler 3. $n := \lceil \log_2 A \rceil$
repeat:
 $x_0, x_1, \dots, x_{n-1} \leftarrow \{0, 1\}$
 $y := \sum_{i=0}^{n-1} 2^i \cdot x_i$
 if $y < A$: return y

Υπόδειξη: Χρησιμοποιήστε την έννοια της δεσμευμένης πιθανότητας.